Microsofte Internet Information Server (IIS)

نویسنده : امیر حسین شریفی

IIS یکی از پر استفاده ترین محیط های کاری برای بسیاری از سرورهای وب در چند سال اخیر بوده است. به همین دلیل همیشه یک هدف عالی برای نفوذگران وب می باشد. این سرور سوراخهای امنیتی بسیار زیادی داشت و دارد و همین امر باعث شده است بسیار مورد حمله نفوذگران وب قرار گیرد از این گونه ضعفهای امنیتی می توان ، ضعفهای امنیتی آشکار سازی کد اصلی برنامه ها شبیه ::$DATA ، آشکار سازی اطلاعات به وسیله اسکریپتهای showcode.asp ، اجرای دستورات سیستمی از طریق تزریق کردن دستورات در پرس و جوهای پلیگاه داده (MDAC / RDS) و حملات سرریزی بافر روی IIS را نام برد. اگر چه این نوع ضعفهای امنیتی توسط پچ هایی که ارائه شده اند و همچنین در نسخه های جدید رفع شده اند البته باید گفت که محصولات جدید ارائه شده با نظم بهتر ارائه شده اند.

بیشتر ضعفهای امنیتی IIS را می توان در دو گروه زیر دسته بندی کرد:

- **حمله علیه مولفه های IIS**
- **حمله علیه خود IIS**

در این مبحث ، هر دو دسته را تا آنجا که بتوانیم توضیح می دهیم و سعی می کنیم با بیان مثالهای متنوعی آنها را بهتر بیان کنیم. البته بیشترین حملات در دسته اول می گنجد .

حمله علیه مولفه های IIS

IIS به صورت خیلی گسترده ای روی مجموعه ای از کتابخانه های دینامیکی (DLL) تکیه کرده است که این مجموعه با یکدیگر تعامل برقرار می کنند تا پروسه های اصلی سیستم را ، inetinfo.exe ، پاسخ دهند و به همین وسیله توانایی های زیادی را برای سیستم ایجاد کرده اند. اگر بخواهید به صورت عملی مجسم کنید ، به صورت ساده ای این فایلهای DLL می تواند توسط یک فایل با یک پسوند اختصاصی از IIS درخواست شود. برای مثال درخواست یک فایل

با پسوند prniter. (البته اگر به صورت حقیقی این فایل موجود باشد) ، از DLL طراحی شده برای درخواستهای چاپ بر پایه وب یک دستگیره[1] درخواست می کند.

این معماری ISAPI [2] ، نامگذاری شده است. پیش پردازنده هائی نظیر ColdFusion و PHP از ISAPI استفاده می نمایند.IIS ، از فیلترهای ISAPI دیگر برای انجام عملیات مرتبط با **ASP** (Active Server Pages) ، **SSI** (Server Side Includes) و اشتراک چاپ مبتنی بر وب ، استفاده می نماید تعداد زیادی از فیلترهای ISAPI ، مستلزم عملیات خاص و جداگانه ای برای نصب نبوده و عملا" بصورت پیش فرض و در زمان نصب IIS بر روس سیستم مستقر (نصب) می گردند همین امر باعث شده بود که نفوذگران بسیاری به وسیله آلوده کردن ورودی های با کد های غیر مجاز از این نوع فایلها سوءاستفاده کنند. آنها خیلی ساده از سرور وب ، توسط URL هایی که به صورت دستی تنظیم شده بود ، یک فایل را درخواست می کردند و ورودی ها را به DLL های ISAPI به وسیله همان درخواست ها تحویل می دادند. تنایج اینگونه درخواستها برای بسیاری از سرورهای IIS فجیع بود! و در این سالهای اخیر به صورت متمادی از این طریق، مورد حمله قرار می گرفته اند.Code red و Code Red 2 ، نمونه هائی از برنامه های مخرب می باشند که از ضعف فوق در جهت پیشبرد اهداف خود استفاده نموده اند . عدم بهنگام سازی و نگهداری مناسب IIS پس از نصب اولیه ، از دیگر مواردی است که زمینه تهاجم برای مهاجمان را فراهم می آورد .مثلا" نقاط آسیب پذیر WebDAV ntdll.dll در IIS 5.0 ، امکان حملات از نوع DoS (غیرفعال نمودن سرویس) را فراهم می کند و مهاجمان در ادامه قادر به ایجاد و اجرای اسکریپت های مورد نظر خود بر روی سرویس دهنده می گردند . در مواردی دیگر و با توجه به نقاط آسیب پذیر موجود ، مهاجمان قادر به اجرای دستورات دلخواه خود بر روی سرویس دهنده می باشند (درخواست دقیق و ماهرانه آدرس های URL) .

امکانات و پتانسیل هائی که در ادامه و با توجه به ضرورت بر روی IIS نصب می گردند (نظیر ColdFusion و PHP) نیز می تواند زمینه بروز نقاط آسیب پذیر جدیدی را فراهم نماید .اینگونه نقاط آسیب پذیر، می تواند بدلیل عدم پیکربندی صحیح و یا وجود ضعف و اشکال امنیتی در محصول نصب شده ای باشد که به IIS نیز سرایت می نماید (توارث مشکلات و ضعف های امنیتی از یک محصول به محصول دیگر) .

مثالهای ابتدایی در زیر آورده شده است و توضیح مختصری درباره آنها بیان شده است. البته اینها جزء مثالهای ابتدایی و اولیه بودند که در سالهای گذشته از آنها سوءاستفاده می کرده اند. اما اجازه بدهید نظری واقعی تر به اینگونه حملات از طریق ISAPI داشته باشیم.

---

1 - Handel
2 - Internet Server Application Programing Interface

سرریزی بافر در ISAPI DLL

یکی از بیشترین حملاتی که روی ISAPI انجام می شود ، حملات سرریزی بافر می باشد.در اواخر سال 2001 و اوایل سال 2002 بسیاری از سرورهای وب IIS توسط کرمهای CodeRed و Nimda ویران شدند. هر دوی این حملات بر پایه سرریزی بافر پیاده سازی شده است که بر اساس سوراخ امنیتی که در ISAPI DLL های منتشر شده روی وب موجود بود آنها را آلوده می کرده اند.در آوریل سال 2002 یکی دیگر از ضعفهای سرریزی بافر روی ISAPI DLL مربوط به صفحات ASP منتشر شد. ما در این بخش از یکی از سوراخهای امنیتی مثالی بیان می کنیم.

در می 2001 ، eEye Digital Security کشف یک سرریزی بافر را درون فیلترهاISAPI ای که فایلهای printer. را به دست می گیرند ، اعلان کرد. این فایلها (C:\WinNT\System32\msw3prt.dll) پروتکل چاپ اینترنت[3] (IPP) را پشتیبانی می کردند. IPP می توانست جنبه های مختلف چاپ از طریق چاپگرهای شبکه را پشتیبانی کند.

این سوراخ امنیتی وقتی به وجود می آید که یک بافر تقریبا 420 بایتی توسط یک سرآمد HTTP Host: برای یک درخواست printer ISAPI. فرستاده شود. اگر در مثال زیر در قسمت [buffer] 420 کاراکتر قرار دهیم این اتفاق خواهد افتاد.

```
GET /NUL.printer HTTP / 1.0
Host: [buffer]
```

این درخواست ساده ، باعث می شود که بافر سرریز شود و IIS بسته می شود. اگر چه ویندوز 2000 به صورت اتوماتیک IIS را دوباره اجرا می کند (Inetinfo.exe) و باعث می شود که IIS سرویسهای وب را به حالتهای اولیه و پیش فرض راه اندازی کند. البته چنین ضعف امنیتی هیچ اثر محسوسی ندارد (به جز اینکه وقتی به صورت دنباله داری ادامه پیدا کند باعث نپذیرفتن سرویسهای اصلی شود) . هنگامیکه IIS دوباره راه اندازی می شود ، باعث می شود که خطاهای تصادفی در IIS رخ دهد و سرور را در حالت نامعلومی قرار دهد!

سوراخ امنیتی افشا سازی منابع (Source Disclosure) در ISAPI DLL

همه سوراخهای امنیتی ISAPI DLL به برجستگی و روشنی **سرریزی بافر** printer. نمی باشد. در این قسمت مثالی درباره ضعف امنیتی **افشا سازی منابع** خواهیم آورد که توسط باگی به وجود آمده است که در ISAPI DLL وجود داشته است. افشا سازی منابع یک رده

3 - Internet Printing Protocol

بزرگ از مباحثی می باشد که به کاربران اطلاعاتی را نمایش می دهد که در حالت عادی ، مجوزی برای نمایش آنها به آن کاربران وجود ندارد.

ضعف امنیتی htr.+ مثال خوبی از افشا سازی کد می باشد که در IIS 4 و 5 وجود دارد. وقتی htr.+ را به یک درخواست فایل فعال می افزاییم ، IIS 4 و 5 ، قطعات داده های منابع فایل را سریعتر از اجرا کردن آن سرویس می دهد ! یعنی قبل از اینکه درخواست توسط IIS اجرا شود ، به صورت متنی ساده نمایش داده می شود. این مثالی می باشد از یک ISAPI DLL که ISM.DLL نامیده می شود و درخواست فوق را به غلط تفسیر می کند. پسوند htr. فایل را به ISM.DLL نگاشت می کند و باعث می شود این فایل یک منبع غلط را تفسیر کند در اینجا یک فایل به نام htr.txt می باشد که شما می توانید با استفاده از Netcat از این سوراخ امنیتی بهره برداری کنید. توجه کنید که htr.+ به درخواست شما بستگی دارد.

```
GET /site1/global.asa+.htr HTTP/1.0
[CRLF]
[CRLF]
```

با استفاده از ارتباطی که به وسیله netcat با یک سرور آسیب پذیر برقرار شده است شما می توانید نتایج را مشاهده کنید:

```
C:\> nc –vv www.victim.com 80 < htr.txt
www.victim.com [10.0.0.10] 80 (http) open
HTTP/1.0 200 OK
Server: Microsoft-IIS/5.0
Date: Thu , 25 Jan 2001 00:50:17 GMT
<!- - filename = global.asa - - > (“Profiles_ConnectString”)
“DSN=profile; UID=company_user; password=secret”
(“DB_ConnectString”) = “DSN=db; UID=company_user; password=secret”
(“PHFConectionString”) = “DSN=phf; UID=sa; PWD=”
(“SiteSearchConnectionString”) = “DSN=SiteSearch; UID=company_user; password=simple”
(“connectionString”) = “DSN=company; UID=company_user; password=guessme”
(“eMail_pwd”) = “sendaemon”
(“LDAPServer”) = “LDAP://directory.company.com:389”
(“LDAPUserId”) = “cn=Directory Admin”
(“LDAPPwd”) = “slapdme”
```

همانطور که مشاهده کردید فایل **global.asa** ، که به صورت معمول برای کاربران نمایش داده نمی شود ، با افزودن **htr.+** به دنباله آن باعث نمایش دادن آن شده است. شما می توانید اطلاعات بسیار سری از کلمات رمزی که در فایل **global.asa** قرار دارد را مشاهده کنید. حال متوجه شدید که با یک اشتباهی که تیم تولید کننده سرور مرتکب شده است چه فاجعه ای رخ داده است!

راههای مقابله با سوراخهای امنیتی ISAPI DLL

ما در اینجا چندین روش مختلف برای شناسایی و پیشگیری از آسیب پذیریهای ISAPI DLL بیان می کنیم و درباره همه آنها مفصل بحث خواهیم کرد.

حذف نگاشت کننده های اضافی بی استفاده

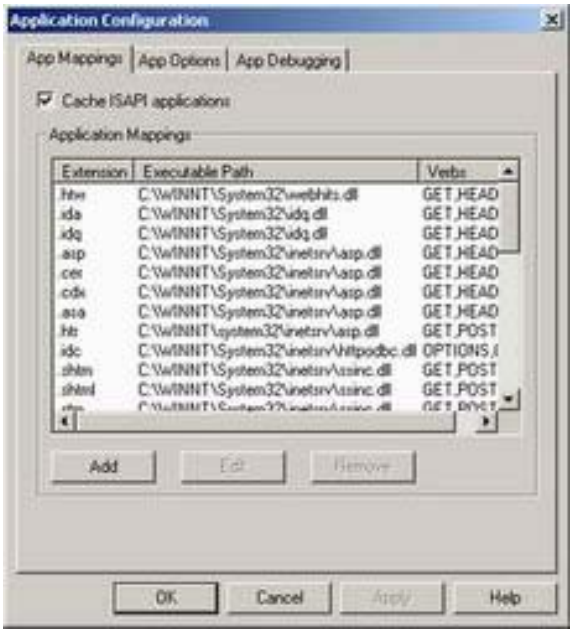
اگر بخواهیم به صورت ریشه ای بیان کنیم ، علت اصلی وجود سوراخهای امنیتی **سرریزی بافر** در **Printer.** و **افشا سازی منابع htr.+** در ISAPI DLL هایی می باشد که باید به در برنامه کاربردی ما غیر فعال باشند و عدم حذف آنها باعث می شود که اطلاعات ورودی روی آنها نگاشت شود و مشکلات عدیده فوق ظاهر گردند. برای حذف آنها باید به صورت پایه های فایلهای DLL ای را که به آنها مربوط می شوند را حذف کرد. همین امر باعث می شود که فایلهای DLL همراه با اجرای IIS به حافظه بار نشوند و برنامه کاربردی ما را از حملات احتمالی محافظت می کند.

« به علت اینکه بیشتر مباحث امنیتی IIS با نگاشتهایی که در فایلهای ISAPI DLL می شود ، ارتباط دارد ، این روش محافظت ، یکی از مهمترین روشهای مقابله با اینگونه حملات می باشد. »

برای غیر فعال کردن DLL ها بر اساس پسوند فایل هایی که باعث نگاشت بر روی این DLL می شوند ، روی Computer ای که شما آن را مدیریت می کنید، کلیک راست کنید و سپس Properties را انتخاب کنید ، سپس موارد زیر را مشاهده می کنید:

- **Master Properties**
- **WWW Service**
- **Edit**
- **Properties of the Default Web Site**
- **Home Directory**
- **Application Setting**
- **Configuration**
- **App Mappings**

مانند شکل زیر ، فایل msw3prt.dll که فایلهای با پسوند .printer روی آن نگاشت می شود را حذف کنید.



البته آسیب پذیریهای زیادی در ISS وجود دارد که همگی به ISAPI DLL های دیگر مربوط می شوند که در جدول زیر بعضی از آنها را به همراه DLL هایی که به آنها نگاشت می شود بیان کرده ایم.

آسیب پذیری	پسوند	اگر نیاز ندارید!
Buffer Overflows, MS02-018	.asp	Active Server Pages functionality
+.htr source disclosure , MS01-004	.htr	Web-based Password reset
آشکار کردن مسیر های دایرکتوری وب ، Q193689	.idc	Internet Database Connector
سرریزی بافر سیستم دور MS01-044	.stm , .shtm , shtml	Server-side include
سرریزی بافر سیستم راه دور ، Ms01-023	.printer	Internet Printer
سرریزی بافر سیستم راه دور ، Ms01-033	.ida , idq	Index Server
Remote IUSR یا سرریزی بافر سیستم MS01-035	Uninstall FPSE RAD Support	FrontPage Server Extension RAD support

نگهداری به وسیله نصب سرویسها Pach و Hotfix میکروسافت

درست است که حذف پتانسیل های آسیب پذیر در نگاشت کننده های ISAPI DLL یک راه حل کامل برای مشکلات ISAPI DLL می باشد ولی راههای مختلف دیگری نیز برای رفع اینگونه مشکلات وجود دارد. از جمله اینکه شما می توانید از Patch هایی استفاده کنید که شرکت میکروسافت برای رفع اینگونه مشکلات آماده کرده است. ابلاغیه های امنیتی میکروسافت[4] به صورت مداوم آسیب پذیریهایی که در ISAPI DLL به وجود آمده است را گزارش کرده است(آنها به وسیله برچسب هایی طبقه بندی شده اند مانند: MS01-026 که نشان دهنده 26 امین ابلاغیه سال 2001 می باشد) در هر کدام از این ابلاغیه های شما می توانید Patch مورد نظر را برای آن آسیب پذیری پیدا کنید.

البته برای سهولت در امر به روز رسانی سرور IIS شما با Patch های جدید، میکروسافت چک کننده Hotfix شبکه[5] (**hfnetchk.exe**) را منتشر کرده است. Hfnetchk تمامی زیر شبکه ها را پویش می کند و گزارش Service Pack و سطح Hotfix را برای هر سیستم ارائه می دهد. البته قبل از اینکه hfnetchk شروع به پویش بکند اطلاعات خود را درباره آخرین Patch های گزارش داده شده توسط میکروسافت ، به روز می کند و این کار را به وسیله XML ای که از پایگاه داده میکروسافت دریافت کرده است ، انجام می دهد.

در صورتیکه از برنامه های اضافه شده ای نظیر CouldDusion، PerlIIS و یا PHP بهمراه IIS استفاده می گردد ، لازم است به سایت های عرضه کنندگان هر یک از محصولات فوق مراجعه کنید و نسبت به آخرین patch ارائه شده در رابطه با هر محصول آگاه و آنان را با توجه به توصیه های انجام شده بر روی سیستم نصب نمایید . امکان Update Windows و سایر سرویس های بهنگام سازی ارائه شده توسط میکروسافت ، شامل Patch های لازم و مرتبط با محصولات اضافه شده سایر شرکت ها در برنامه IIS مایکروسافت نبوده و لازم است مدیران سیستم بهنگام سازی محصولات اضافه شده (غیر میکروسافت) در IIS را خود راسا" انجام دهند .

استفاده از IISLochdown و URLScan

در اواخر سال 2001 ، میکروسافت ابزاری به نام **ISSLockdown Wizard** را منتشر کرد و همانطور که از نامش مشخص است ، یک ابزار خودکار می باشد برای پیکربندی IIS بر پایه مسایل امنیتی آن. با اجرای برنامه فوق در حالت " Custom " و یا " "Expert ، می توان تغییرات

4 - Microsoft Security Bulletine
5 - Network Hotfix Checker

مورد نظر خود را در ارتباط با نصب IIS مشخص نمود. بدین ترتیب ، امکان اعمال تغییرات زیر در رابطه با نصب IIS ، فراهم می گردد :

- **سرویسهای اینترنت:** اجازه می دهد کلیه سرویس های ISS را غیر فعال کنید. (WWW ، FTP ، SMTP و NNTP) البته بسته نقشی که سرویس دهنده شما دارد.
- **مسایل امنیتی اضافی :** غیر فعال نمودن WebDAV (مگر اینکه محیط مورد نظر شما به وجود آن برای نشر محتوی وب ، نیاز داشته باشد) و حذف نمونه برنامه های ارائه شده بهمراه IIS و همچنین منع سرویس دهنده وب از اجراء دستورات سیستمی متداول که عموما" توسط مهاجمان استفاده می گردد(نظیر cmd.exe و یا tftp.exe) .
- **Script Maps** : غیر فعال نمودن ISAPI extensions های غیر ضروری (نظیر : htr. ، idq . printer. ، ism. ,)
- **UrlScan** : ابزاری برای فیلتر نمودن درخواستهای داده شده به IIS و نپذیرفتن آنها در صورتی که آنها از مشخصات خاصی پیروی می کردند!

نمونه های بالا یک لیست تقریبا خوبی از راههای پیکربندی مخصوص IIS می باشد ، البته بعضی مسایل از قلم افتاده است. IISLockdown درباره نصب Service Pack و Hotfix ها هیچ کاری انجام نمی دهد ، همچنین هیچ محافظت و عملکردی درباره جنبه های دیگر سیستم عامل ویندوز ندارد و یا هیچ دیوار آتشی در جلو سرویس دهده وب ما ایجاد نمی کند. IISLockdown یک ابزار مختصر و ساده می باشد و نمی توان به طور کامل روی آن تکیه کرد و از جنبه های دیگر غافل شد.

از میان چیزهایی که IISLockdown به صورتی دستی پیکر بندی می کند ، یکی از آنها خیلی نمایان است ، **URLScan** !

البته URLScan می تواند به صورت جداگانه ای از روی نصب کننده IISLockdown (iislock.exe) نصب شود. شما می توانید با دستور زیر این کار را انجام دهید:

```
C:\> iislock.exe  /q  /c  /t : c:\lockdown_files
```

البته روش دیگر برای نصب URLScan از طریق IISLockdown Wizard می باشد که به صورت خودکار می تواند نصب شود.

URLScan شامل دو فایل URLScan.dll و URLScan.ini می باشد که باید در همان دایرکتوری نصب ، قرار گیرد. URLScan.dll یک فیلتر ISAPI می باشد که باید جلو IIS قرار گیرد و مانند یک حائل عمل کند و قبل از اینکه IIS درخواستها را دریافت کند ، بتواند آنها را

تحلیل کند و URLScan.ini یک فایل پیکربندی می باشد و تصمیم می گیرد که چه نوع درخواستهای HTTP نباید توسط URLScan ISAPI پذیرفته شود. درخواست های پذیرفته نشده در یک فایل به نام URLScan.log در همان دایرکتوری نصب ذخیره می شود. (البته فایل های ثبت گزارش ممکن است به نام URLScan.MMDDYY.log ذخیره شود) URLScan برای درخواستهای که رد می کند پاسخ HTTP 404 Object not found را می فرستد.

می توان با پیکربندی URLScan تمامی درخواستهای HTTP ای را که بر پایه موارد زیر می باشند نپذیرفت:

- بر اساس روشهای درخواست (یا کلمات ، مانند GET ، POST ، HEAD و غیره)
- بر اساس پسوند فایلهای درخواست شده
- بر اساس URL های رمزشده مشکوک (در مباحث بعدی خواهید دید که این قسمت چقدر مهم می باشد!)
- بر اساس حضور کاراکترهای non-ASCII در URL ها
- بر اساس حضور ترتیب خاصی از کاراکترها
- بر اساس حضور سرآمدهای مخصوص در درخواستها

برای هر کدام از این موارد پارامترهای مشخص وجود دارد که باید طبق یک ضوابطی در فایل URLScan.ini گذاشته شوند.

نکته: URLScan.ini فقط در زمان اجرا شدن IIS می تواند بارگذاری شود و هر گونه تغییراتی در آن فقط زمانی اعمال می شود که IIS دوباره راه اندازی شود.

پیاده سازی یک فیلتر کننده درزهای شبکه

اولین چیزی که معمولا به ذهن یک هکر می آید این است که به چه صورت می تواند دستورات را در سرور به اجرا دربیاورد تا بتواند به سرور تسلط پیدا کند و فایلهایی را از خارج به سرور وارد کند . حال می توان با قرار دادن یک فیلتر کننده خروجی به وسیله دیواره آتش در مقابل سرور وب جلو تمامی خروجی هایی را که می خواهند به پورتهای دیگر ارتباط برقرار کنند ، بگیریم. یک راه ساده آن است که تمامی ارتباطات از داخل به بیرون از شبکه را رد کنیم به جز آنهایی که از قبل قرار داده ایم و این کار، با بلوکه کردن تمامی درخواستهایی انجام می شود که فقط یک پرچم TCP SYN [6] دارند. البته با این کار پاسخهایی که به درخواستهای مشروع که به

6- همانطور که می دانید برای برقراری یک ارتباط به روش **دست تکانی سه مرحله ای** ، در مرحله اول ابتدا یک بسته TCP درست می شود که فیلد SYN آن مقدار یک دارد!

داخل می آیند بلوکه نمی شوند و برای سرور این امکان را ایجاد می کند که بتواند به بیرون دسترسی داشته باشد. (درست گفتم ؟!)

دیده بانی و ثبت وقایع

یکی دیگر از روشهای مقابله فهمیدن این موضوع است که ، وقتی یک نفوذگر در تدارک یک حمله به زیر و بم ISAPI DLL می باشد ، دنبال چه چیزی می گردد . دو تا از ویران کننده ترین نتایج **سرریزی بافر** در نگاشت کننده ها روی پسوند های ida/idq ISAPI بود که باعث تولد گونه جدیدی از کرمهای اینترنتی به نام Code Red و Nimda گردید. این کرمها همانند ویروس ها خودشان را منتشر می کردند و در اواخر سال 2001 و تا اوایل 2002 بسیاری از سرورهای آسیب پذیر از این سرریزی بافر را آلوده کردند. فایل ثبت وقایع سرورهایی که آلوده شده بودند به کرم Code Red محتوی مدخلی شبیه به زیر بودند:

```
GET    / default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u78
01%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00
%u531b%u53ff%u0078%u0000%u00=a
```
[7]

Code Red و Nimda همچنین تعدادی فایل را در سیستم های آلوده ایجاد می کنند . به عنوان مثال حضور دایرکتوری %System%\notworm نشان دهنده این موضوع می باشد که سیستم در حال حاضر به کرم Code Red آلوده می باشد. همچنین است حضور فایل root.exe که فایل دستورات شل ویندوز می باشد که به این نام تغییر پیدا کرده است ، نشان دهنده این است که سیستم آلوده به کرم Nimda می باشد

پس باید به صورت منظمی فایل های ثبت وقایع را بررسی کنید و همچنین فایل های سرور را بازبینی کنید تا در صورت برخورد با موارد مشکوک آنها را پیگیری کنید. همه این نکات به شما کمک می کند که یک سرور امنی داشته باشید.

داده های پنهانی را در کد منابع[8] اتان قرار ندهید

7- نکته ای که اینجا می باشد این است که مهاجم دستورات اسمبلی را به یونیکد رمزگذاری کرده است. برای مثال %u9090 به 0x90 0x90 تبدیل می شود که هر کدام در زبان ماشین x86 به معنی دستور NOP می باشد !

8 - Source Code

آنچه که مشخص است IIS مشکل افشا سازی کد را دارد. این فرض غلطی می باشد که فکر کنید هیچ کس قادر به دیدن کدهای منابع شما نمی باشد! برنامه نویس ها باید یاد بگیرند که مرتکب چنین اشکالی نشوند بعضی از عمومی ترین خطاها شامل موارد زیر می باشد:

- رشته های با متون واضح و روشن برای ارتباط با پایگاه داده به وسیله دستورات SQL که در اسکریپتهای ASP نوشته می شوند.
- کلمات رمزی که به صورت متون ساده و روشن در فایل global.asa به کار می رود.
- استفاده از فایلهای include با پسوند های inc. ، که می توان آنها را با پسوند asp. به کار برد و در اسکریپتهای دیگر نیز این تغییر نام را اعمال کرد.
- توضیحات درون اسکریپتها که محتوی اطلاعات مخفی می باشد مانند آدرس ایمیل ، اطلاعاتی درباره ساختمان دایرکتوریها ، کلمات رمز و ...

به صورت منظم شبکه خود را برای پیدا کردن آسیب پذیریها پویش کنید

شاید یکی از بهترین روشهای محافظت از چنین حملاتی این است که به صورت منظم سرور را پویش کنید تا به نقاط آسیب پذیری که مهاجمان از آنها بهره می برند آگاه شوید. پس قبل از اینکه دیگران این کار را علیه شما انجام دهند ، خودتان دست به کار شوید و آسیب پذیریهای سیستم خود را پیدا کرده و در جهت رفع آنها اقدام کنید.

در مباحث بعدی درباره اینگونه پویشگرها به طور مفصل بحث خواهیم کرد.

پاسخ آسیب پذیر قابل پیش بینی	HTTP GET	آسیب پذیریهای مشهور
200 OK(/default.asp source must be present)	/default.asp+.htr	+.htr source disclosure, MS01-004
500 Error performing query	/null.idc	Web directory path disclosure,Q193689
200 OK (/file.stm must be present)	/file.stm,.shtm,.shtml	Server side includes buffer overflow
500 Internal server error; HTML contains **Error in Web printer install**	/null.printer	.printer buffer overflow,MS01-023
200 OK; HTML contains **The IDQ file .. could not be found**	/null.ida,idp	Index Server buffer overflow,MS01-033
200 OK; HTML contains **The format of QUERY_STRING is invalid**	/null.htw	**Webhits** source disclosure,MS00-006
501 Not Implementd	/_vti_bin/_vti_aut/fp30reg.dll	FrontPage Server Extension buffer overflow,MS01-035

منابع :

1- **Hacking Exposed – Web Application** , JOEL SCAMBRAY , MIKE SHEMA
2- **Web Hacking - Attacks and Defense**, Stuart McClure, Saumil Shah, Shreeraj Shah
3- www.SRCO.ir